Tietopalvelut
Sote-tieto ja -tiedonhallinta

9.12.2021

MÄÄRÄYS SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN OLENNAISISTA TOIMINNALLISISTA JA TIETOTURVAVAATIMUKSISTA

Valtuutussäännökset

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021, jäljempänä asiakastietolaki) 29 §:n 4 momentti, 32 §:n 4 momentti, 34 §:n 4 momentti ja 35 §:n 3 momentti, 9 §:n 2 momentti.

Kohderyhmät

Sosiaali- ja terveydenhuollon tietojärjestelmäpalvelujen tuottajat ja tietojärjestelmien valmistajat
Kanta-välityspalvelujen tuottajat
Sosiaali- ja terveydenhuollon palvelunantajat
Apteekit
Kansaneläkelaitos
Tietoturvallisuuden arviointilaitokset
Välittäjät

Voimaantulo

Määräys tulee voimaan 9. päivänä joulukuuta 2021 ja se on voimassa toistaiseksi.

Määräyksellä 4/2021 on kumottu aiemmat määräykset THL 1/2015 ja 2/2016, joissa on ollut myös tämän määräyksen (5/2021) aihesisältöjä. Aiemmat määräykset on annettu asiakastietolain 159/2007 nojalla. Lailla 784/2021 on kumottu laki 159/2007.

Sisällys

1 Määräyksen tarkoitus

Tämän määräyksen tarkoitus on täsmentää sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyyn tarkoitettuihin tietojärjestelmiin kohdistuvat olennaiset vaatimukset, jotta niiden tarkoituksenmukainen toiminta, yhteensopivuus ja tietoturvallisuus voidaan varmistaa.

2 Määräyksen soveltamisala

Tämä määräys koskee sosiaali- ja terveydenhuollon asiakas- tai potilastietoja käsittelevien tietojärjestelmien olennaisten vaatimusten sisältöä (asiakastietolain 7 luku "Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset"). Terveyden ja hyvinvoinnin laitoksella (jäljempänä THL) on asiakastietolain 34 §:n 4 momentin perusteella valtuus antaa tarkempia määräyksiä olennaisten vaatimusten sisällöstä ja siitä, mitkä olennaiset vaatimukset on täytettävä eri palveluissa käytettävissä tietojärjestelmissä ja 35 § perusteella valtuus antaa määräyksiä vaatimustenmukaisuuden osoittamisessa noudatettavista menettelyistä ja annettavan selvityksen sisällöstä.

Tämä määräys koskee:

- valtakunnallisiin tietojärjestelmäpalveluihin (Kanta-palvelut) liitettäviksi tarkoitettuja asiakas- ja potilastietoja käsitteleviä tietojärjestelmiä ja muita käyttötarkoituksensa perusteella sertifioitavia tietojärjestelmiä ja välittäjien palveluja (luokka A1, A2 ja A3) ja

- muita sosiaali- ja terveydenhuollon järjestelmiä, joiden käyttötarkoituksena on asiakas- ja potilastietojen käsittely (luokka B).

Määräyksen mukaisten olennaisten vaatimusten käyttökohteita ovat:

- asiakas- tai potilastietojärjestelmien tai osajärjestelmien käyttötarkoituksen kuvaaminen ja viestintä;

- kansallisesti asetettavien vaatimusten kokoaminen sekä vaatimuksia tarkemmin kuvaavien määritysten löytäminen ja niihin viittaaminen;

- Kanta-palveluihin liittyvissä luokan A2 ja A3 tietojärjestelmissä Kelan Kanta-palvelujen yhteistestauksessa ja sen eri testauskokonaisuuksissa läpikäytävien vaatimusten selkeyttäminen;

- järjestelmän valmistajan oman toiminnallisen testauksen tukeminen ennen yhteistestaukseen hakeutumista;

- tietojärjestelmien valmistajien ja tietojärjestelmäpalvelujen tuottajien omassa testauksessa, Kelan yhteistestauksessa sekä mahdollisissa asiakastestauksissa testattavien järjestelmäominaisuuksien ryhmittely;

- tietoturvallisuuden arviointiin liittyvien tietoturvavaatimusten kuvaaminen tietoturvallisuuden arviointeja varten;

- samoihin toiminnallisiin tai asiallisiin kokonaisuuksiin liittyvien vaatimusten ja määritysten ryhmittely ja linkittäminen;

- eri ajankohtina voimassa olevien määritysten kokoaminen tietyn toiminnon tai tietosisällön toteuttamiseksi;
- tiettyyn tarkoitukseen tarkoitettujen järjestelmien pakollisten vaatimusten ilmaiseminen;
- pakollisten vaatimusten aikataulujen ja siirtymäaikojen selkeyttäminen (esimerkiksi asiakastietolaissa asetettujen siirtymäaikojen ja tiettynä vuonna voimassa olevien määritysten ja olennaisten vaatimusten suhteen);
- tuki kansallisesti asetettavien olennaisten vaatimusten kuvaamiseen ja huomiointiin tietojärjestelmien suunnittelussa ja toteuttamisessa sekä tietojärjestelmien hankinnoissa;
- tietojärjestelmäkokonaisuuksissa ja modulaarisissa tietojärjestelmissä eri osajärjestelmien sisältämien ominaisuuksien kuvaaminen; sekä
- käytettävän käsitteistön ja vaatimusten yhdenmukaistaminen järjestelmien valmistajiin, tietojärjestelmäpalvelujen tuottajiin ja niiden käyttäjiin kohdistuvissa vaatimuksissa, jotka perustuvat säädöksiin ja valtakunnallisiin määrityksiin.

3 Määräyksen keskeinen sisältö ja rajaukset

Asiakastietolain mukaan asiakas- tai potilastietojen käsittelyssä käytettävän tietojärjestelmän tulee täyttää yhteentoimivuutta, tietoturvaa ja tietosuojaa sekä toiminnallisuutta koskevat olennaiset vaatimukset. Vaatimusten täyttämisestä tietojärjestelmässä vastaa tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja.

Asiakastietolaissa säädetään myös siitä, että palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Tämä määräys täsmentää sitä, miten palvelunantajan käyttämissä tietojärjestelmissä olennaisten vaatimusten täyttäminen varmistetaan.

Asiakastietolain mukaan sosiaali- ja terveydenhuollon tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan on osoitettava järjestelmän tai palvelun vaatimustenmukaisuus. Osoittamiseen kuuluu selvitys siitä, että järjestelmä täyttää ne olennaiset vaatimukset, jotka vastaavat sen käyttötarkoitusta. Selvitys annetaan määräyksen 4/2021 ja tämän määräyksen mukaisesti.

Tämän määräyksen liitteenä on kansallisesti yhdenmukainen sosiaali- ja terveydenhuollon tietojärjestelmien olennaisten vaatimusten luokitus (Liite 2). Luokitus sisältää sosiaali- ja terveydenhuollon asiakas- ja potilastietojen käsittelyssä käytettävien tietojärjestelmien olennaisten vaatimusten ylätason kuvaukset. Määräyksessä myös täsmennetään se, mitkä olennaiset vaatimukset eri käyttötarkoituksiin tarkoitetuissa järjestelmissä tulee vähintään toteuttaa tai täyttää (Liitteet 3). Lisäksi tässä määräyksessä tarkennetaan olennaisten vaatimusten kuvaamisessa, todentamisessa ja hyödyntämisessä käytettäviä menettelyjä.

Määräys koskee sekä Kanta-palveluihin liittyviä että muita asiakas- ja potilastietojen käsittelyyn kuuluvia järjestelmiä, jotka kuuluvat luokkaan A tai luokkaan B. Useat vaatimuksista ja niiden perusteena olevista määrityksistä koskevat Kanta-palveluihin liittyviä luokkaan A2 tai A3 (ks. määräys 4/2021) kuuluvia järjestelmiä.

Määräyksessä käytetyt termit ja rajaukset vastaavat määräyksessä 4/2021 käytettäviä termejä ja rajauksia.

Määräyksen ja sen liitteiden valmisteluun ovat osallistuneet Terveyden ja hyvinvoinnin laitoksen (THL), Kansaneläkelaitoksen (Kela), Sosiaali- ja terveysalan lupa- ja valvontaviraston (Valvira), Sosiaali- ja terveysministeriön (STM), Liikenne- ja viestintäviraston (Traficom) sekä sosiaali- ja terveydenhuollon palvelunantajien kehittämisprojektien asiantuntijat. Määräyksessä on huomioitu aiempien säädösten soveltamisen yhteydessä tunnistettuja kehittämistarpeita.

Ennen tämän määräyksen antamista Terveyden ja hyvinvoinnin laitos on järjestänyt lausuntokierroksen kuullakseen asianomaisia sidosryhmiä. Kuulemisten tulokset on huomioitu määräyksessä ja sen liitteissä.

4 Suhde muihin määräyksiin, ohjeisiin ja määrityksiin

THL on antanut määräyksen sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista (THL:n määräys 4/2021: määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista). Tämä määräys täsmentää määräyksessä 4/2021 kuvatuilla menettelyillä todennettavat vaatimukset ja erityyppisten vaatimusten mukaisuuden ilmoittamisessa ja todentamisessa käytettävät menettelyt.

THL on antanut erillisen määräyksen 1/2021 sosiaalihuollon asiakasasiakirjoista ja niihin merkittävistä tiedoista.

THL:n määräyksessä 3/2021 kuvataan sote-palvelunantajilta, välittäjiltä sekä Kelalta edellyttettävään tietoturvasuunnitelmaan sisällytettävät selvitykset ja vaatimukset. Osana tietoturvasuunnitelmaa kuvataan, kuinka palvelunantaja osaltaan varmistaa tuotantokäytössä toimivien tietojärjestelmien vaatimustenmukaisuuden osana tietoturvasuunnitelmaa ja sen kautta tapahtuvaa omavalvontaa.

Tämän määräyksen liitteessä 2 oleva olennaisten vaatimusten luokitus viittaa useisiin tarkempiin määrityksiin ja ohjeisiin, joissa kuvataan yksityiskohtaisia toiminnallisia ja tietosisältöihin kohdistuvia vaatimuksia. Luokitus on tarkoitettu selkeyttämään ja tukemaan tietojärjestelmien ja palveluiden kehittämistä, sertifiointia, testausta, tietoturvallisuuden arviointia, hankintaa ja eri osapuolten välistä viestintää. Määräyksen soveltamisessa luokitus toimii myös hakemistona, jonka kautta keskeisimmät kansallisia vaatimuksia kuvaavat määritykset ovat löydettävissä.

Määräyksessä ja sen liitteissä kuvatut olennaiset vaatimukset korvaavat aiemman asiakastietolain sekä määräysten 1/2015 ja 2/2016 nojalla asetetut olennaiset vaatimukset. Suuri osa olennaisista vaatimuksista on samoja kuin aiemmissa määräyksissä.

Tätä määräystä ei sovelleta tietojärjestelmiin, joiden käyttötarkoituksena ovat pelkästään Sosiaali- ja terveysalan tietolupaviranomaisen (Findata) antaman määräyksen 1/2020 (Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista) mukaiset käyttökohteet. Kyseistä määräystä sovelletaan kaikkiin niihin toisiolaissa säädettyihin käyttötarkoituksiin, joihin toisiolain mukaan tarvitaan tietolupa: tieteellinen tutkimus, tilastointi, opetus sekä viranomaisen suunnittelu- ja selvitystehtävä.

5 Olennaiset toiminnalliset vaatimukset

Olennaiset toiminnalliset vaatimukset koskevat tietojärjestelmiin toteutettavia toimintoja ja tietosisältöjä. Olennaisia toiminnallisia vaatimuksia ovat tämän määräyksen liitteessä 2 (Olennaisten vaatimusten luokitus) kuvatut toiminnot ja tietosisällöt, jotka viittaavat erillisiin tarkempiin määrityksiin. Näissä tarkemmissa määrityksissä kuvataan tarkemmin myös pakollisia ja vapaaehtoisia toimintoja ja tietoja.

Monet olennaiset toiminnalliset vaatimukset keskittyvät tässä määräyksessä niihin toiminnallisuuksiin ja tietoihin, jotka ovat keskeisiä Kanta-palveluihin suoraan tai välillisesti liittyvien tietojärjestelmien näkökulmasta.

6 Olennaiset tietoturvavaatimukset

Olennaiset tietoturvavaatimukset koskevat tietojärjestelmiin toteutettavia ja niiden kautta täytettäviä tietoturvallisuuden ja tietosuojan varmistamiseksi toteutettuja ominaisuuksia ja tietojärjestelmän tai osajärjestelmän suunnittelussa, toteuttamisessa tai tarjoamisessa tarvittavia toimenpiteitä. Olennaisia tietoturvavaatimuksia ovat tämän määräyksen liitteessä 2 (Olennaisten vaatimusten luokitus) kuvatut tietoturvavaatimukset. Osa vaatimuksista viittaa erillisiin tarkempiin määrityksiin.

Olennaisten vaatimusten luokituksessa Tietoturvavaatimukset-välilehdellä kohdissa ”Otsikko” ja ”Selite” esitettävät vaatimukset ovat sitovia vaatimuksia. Kunkin vaatimuksen toteutuminen on todennettava osana tietoturvallisuuden arviointia luokkaan A kuuluvassa tietojärjestelmässä vaatimukselle määritellyn todentamistavan mukaisesti, jos vaatimus on järjestelmän käyttötarkoituksen näkökulmasta relevantti. Todentaminen osana sertifiointiprosessia tapahtuu määräyksen 4/2021 mukaisesti.

Tietojärjestelmäpalvelun tuottajan on otettava kantaa siihen, mitkä tietojärjestelmän käyttöympäristön olennaisista tietoturvavaatimuksista toteutuvat tietojärjestelmän tai siihen liittyvien tietojärjestelmäpalvelun tuottajan palvelujen kautta, ja mitkä käyttöympäristön vaatimuksista ovat tietojärjestelmää käyttävän palvelunantajan vastuulla (ks. luku 9). Vaatimukset, jotka sisältyvät tietojärjestelmään tai tietojärjestelmäpalvelun tuottajan palveluun, todennetaan osana tietoturvallisuuden arviointia. Todentamisessa ja sertifioinnissa ei edellytetä palvelunantajaorganisaation osallistumista käyttöympäristöön kohdistuvien vaatimusten todentamiseksi.

7 Vähimmäisvaatimusten profiilit

Tiettyyn käyttötarkoitukseen tarkoitetun tietojärjestelmän, osajärjestelmän tai tietojärjestelmäkokonaisuuden vähimmäisvaatimukset voidaan ilmaista kansallisen vähimmäisvaatimusprofiilin (profiili) avulla. Yksi profiili sisältää osajoukon olennaisten vaatimusten luokituksessa kuvatuista toiminnoista ja tietosisällöistä. Määräyksen liitteissä 3a-3g on profiileja, jotka kokoavat yhteen useisiin sosiaali- ja terveydenhuollon tietojärjestelmien käyttötarkoituksiin kansallisesti asetettavat vähimmäisvaatimukset. Kussakin liitteessä on yksi tai useampia profiileja.

Profiilin mukaiset olennaiset vaatimukset on toteutettava tai täytettävä tietojärjestelmässä, jonka käyttötarkoitukseen sisältyy profiilissa kuvattu käyttötarkoitus. Profiilin mukaisten vähimmäisvaatimusten toteuttaminen on edellytyksenä tiettyyn käyttötarkoitukseen käytettävän tietojärjestelmän tai tietojärjestelmäkokonaisuuden hyväksymiselle tuotantokäyttöön. Tämän määräyksen liitteenä olevat profiilit ovat sitovia.

Tietojärjestelmäpalvelun tuottajan on ilmoitettava kaikki ne valtakunnalliset vähimmäisvaatimusten profiilit, joiden mukainen käyttötarkoitus tietojärjestelmään sisältyy. Poikkeuksena ovat profiilit, joiden kuvauksessa on erikseen ilmaistu, että kyseistä profiilia ei tarvitse erikseen ilmoittaa, jos järjestelmä täyttää jonkin toisen (laajemman) profiilin mukaiset vaatimukset[1]. Ilmoittaminen tehdään osana luokan A tietojärjestelmän sertifiointia ja osana luokan A tai luokan B tietojärjestelmän käyttötarkoituksen kuvaamista ja rekisteröintiä määräyksen 4/2021 mukaisesti käyttäen tämän määräyksen liitteenä 4 olevaa järjestelmälomaketta:

[1] Määräyksen 5/2021 voimaan tullessa profiili 3g1 (liitteessä 3g) on tällainen profiili, jonka sisältämiin vaatimuksiin on otettu kantaa kaikissa liitteiden 3a-3f mukaisissa profiileissa. Tässä tapauksessa järjestelmälomakkeessa ei tarvitse erikseen ilmoittaa profiilia 3g1, jos järjestelmä täyttää jonkin muun profiilin mukaiset vaatimukset.

1. kun luokan A2 tai A3 järjestelmä hakeutuu Kelan kanssa suoritettavaan yhteistestaukseen,

2. kun luokan A1, A2 tai A3 järjestelmä hakeutuu tietoturvallisuuden arviointiin,

3. kun luokan B, A1, A2 tai A3 järjestelmän rekisteröidään Valviran tietojärjestelmärekisteriin.

Yksi tietojärjestelmä, osajärjestelmä tai tietojärjestelmäkokonaisuus voi täyttää myös useiden profiilien mukaiset vaatimukset. Järjestelmään on oltava toteutettuna ja järjestelmälomakkeelle merkittynä ne olennaiset vaatimukset, jotka ovat pakollisia järjestelmän käyttötarkoitusta vastaavissa vähimmäisvaatimusten profiileissa.

Tietyn profiilin mukaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän tai osajärjestelmän kautta. Tällöin ilmoituksissa ja sertifioinnissa on kuvattava, minkä muiden tietojärjestelmien tai osajärjestelmien kanssa käytettynä tietojärjestelmä tai tietojärjestelmäpalvelu täyttää profiilin mukaiset vaatimukset, ja mitä muita edellytyksiä vaatimusten täyttämiselle on.

Järjestelmän käyttötarkoitukseen sisältyvien profiilien edellyttämien vaatimusten toteuttaminen tai täyttäminen sekä niiden todentaminen yhteistestauksessa tai tietoturvallisuuden arvioinnissa siltä osin kuin vaatimukset ovat sertifioinnissa todennettavia on edellytys luokan A tietojärjestelmien hyväksytylle sertifioinnille ja tuotantokäyttöönotolle.

Valviran ylläpitämässä tietojärjestelmien rekisterissä ilmoitetaan kunkin tietojärjestelmän tai osajärjestelmän käyttötarkoitukseen sisältyvät profiilit.

Mikäli kyseessä on luokan A tietojärjestelmä, rekisteröinti Valviran tietojärjestelmärekisteriin edellyttää sitä, että profiilin mukaisiin toimintoihin liittyvät yhteentoimivuuden ja tietoturvallisuuden vaatimukset on hyväksytysti todennettu yhteistestauksessa ja tietoturvallisuuden arvioinnissa ja että tietojärjestelmä on saanut tietoturvallisuustodistuksen. A-luokan järjestelmissä vaatimusten täyttyminen on tarvittaessa todennettava osana sertifiointia myös silloin, kun vaatimuksia täytetään muiden tietojärjestelmien tai osajärjestelmien kautta.

Tiettyyn käyttötarkoitukseen tarkoitettujen tietojärjestelmien vähimmäisvaatimuksista voidaan myös antaa erillisiä määräyksiä, jotka viittaavat luokituksen avulla määriteltyihin profiileihin.

Profiilien käyttöä ja suhdetta olennaisiin vaatimuksiin kuvataan myös Liitteessä 1.

8 Olennaisten vaatimusten täyttäminen / tietojärjestelmäpalvelun tuottaja

Tietojärjestelmäpalvelun tuottaja käyttää olennaisten vaatimusten täyttämisen osoittamiseen Liitteessä 4 olevaa järjestelmälomaketta, jonka avulla määräyksen 4/2021 mukaisesti tietojärjestelmää koskevia tietoja ilmoitetaan järjestelmien sertifioinnissa ja rekisteröinnissä. Kaikki tietojärjestelmään tai osajärjestelmään toteutetut olennaiset vaatimukset kuvataan yhdellä järjestelmälomakkeella. Tämän luvun tietojärjestelmiä koskevia kohtia voidaan soveltaa myös osajärjestelmiin, joita voidaan sertifioida osana laajempaa tietojärjestelmäkokonaisuutta.

Luokan B tietojärjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

1. tietojärjestelmäpalvelun tuottaja on kuvannut tietojärjestelmän käyttötarkoituksen, luokitellut järjestelmän ja arvioinut järjestelmän riskitason määräyksen 4/2021 mukaisesti;

2. tietojärjestelmäpalvelun tuottaja on yksilöinyt järjestelmälomakkeeseen ne olennaisten vaatimusten profiilit (Liite 3), jotka ovat osa tietojärjestelmän käyttötarkoitusta;

3. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisten vaatimusten toiminnot, joiden mukaisia toiminnallisuuksia järjestelmään sisältyy;

4. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisten vaatimusten tietosisällöt, joita järjestelmässä käsitellään, ilmaisten sen mitä tietoja järjestelmä tuottaa tai käyttää;

5. tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmälomakkeeseen ne olennaisiin vaatimuksiin sisältyvät tietoturvavaatimukset, jotka järjestelmässä toteutetaan tai sen kautta täytetään;

6. kohtien 3-5 mukaisesti merkityt vaatimukset sisältävät vähintään järjestelmää koskevien profiilien mukaiset vaatimukset;

7. kohtien 3-5 mukaisiin vaatimuksiin on järjestelmälomakkeessa ohjeistetulla tavalla merkitty a) ne vaatimukset, jotka järjestelmässä täytetään muiden tietojärjestelmien tai osajärjestelmien avulla sekä b) ne vaatimukset, joihin liittyen järjestelmässä on tehty merkittäviä muutoksia, mikäli tällaisia vaatimuksia on;

8. tietojärjestelmän valmistaja tai tietojärjestelmäpalvelun tuottaja on *itse testannut ja todennut järjestelmässä toimivaksi* kohtien 3-7 mukaiset olennaiset vaatimukset.

Luokan A1 tietojärjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

9. luokan B mukaiset edellytykset (yllä) on täytetty;

10. järjestelmää koskevat olennaiset tietoturvavaatimukset (kohta 5) on *toteutettu, täytetty ja dokumentoitu* siten, että järjestelmälle voidaan suorittaa tietoturvallisuuden arviointi ja antaa todistus hyväksytystä tietoturvallisuuden arvioinnista.

Luokan A1, A2 tai A3 tietojärjestelmän tuotantokäyttöönotto edellyttää sitä, että yllä kuvattu todennettuja tietoturvavaatimuksia koskeva tietoturvallisuustodistus on annettu ja sitä vastaavat tiedot löytyvät Valviran tietojärjestelmärekisteristä (ks. myös määräys 4/2021 luku 9).

Luokan A2 tai A3 tietojärjestelmä täyttää siihen kohdistuvat olennaiset vaatimukset, kun:

11. luokan A1 mukaiset edellytykset (yllä) on täytetty;

12. järjestelmälomakkeeseen on merkitty käsiteltävien tietosisältöjen (kohta 4) osalta, mitä tietoja järjestelmä tuottaa Kanta-palveluihin tai hyödyntää Kanta-palveluista;

13. Kanta-palveluihin liittyviin määrityksiin liittyvät järjestelmää koskevat toiminnalliset vaatimukset (toiminnot ja tietosisällöt, kohdat 3-8), on *toteutettu, täytetty ja dokumentoitu* siten, että järjestelmälle voidaan hyväksytysti suorittaa tarvittavat yhteistestaukset Kelan Kanta-palvelujen yhteistestauksen ohjeiden mukaisesti.

Edellä kuvattujen seikkojen ilmoittamista järjestelmälomaketta käyttäen kuvataan määräyksen 5/2021 liitteen 1 luvussa 2.3.

Luokan A2 tai A3 tietojärjestelmän tuotantokäyttöönotto edellyttää sitä, että kaikki järjestelmän Kanta-palveluihin liittyvät toiminnot ja tietosisällöt, joihin kohdistuu yhteistestauksen sisältöjä, on hyväksytysti yhteistestattu (ks. myös määräys 4/2021 luku 9).

Luokkaan A kuuluvan tietojärjestelmän vaatimustenmukaisuus on osoitettava sertifioinnilla ennen tuotantokäyttöönottoa. Olennaiset vaatimukset täyttävä luokan A tai B tietojärjestelmä on rekisteröitävä Valviran tietojärjestelmärekisteriin. Sertifioinnin ja rekisteröinnin prosessi kuvataan määräyksessä 4/2021 ja tämän määräyksen liitteessä 1. Edellä mainittujen edellytysten numerointi ei suoraan vastaa sertifiointi- ja rekisteröintiprosessin vaiheita.

Mikäli luokan A järjestelmä ilmoitetaan yhteistestaustarpeen uudelleenarviointiin tai arviointiin siitä, tarvitaanko järjestelmälle uusi tietoturvallisuuden arviointi, on uudet ja olennaisia muutoksia sisältävät toiminnot ja tietosisällöt merkittävä selkeästi Liitteen 4 mukaiseen järjestelmälomakkeeseen.

Tämän määräyksen mukainen järjestelmälomake sekä asiakastietolain edellyttämä selvitys ja ilmoitus on tehtävä riippumatta siitä, täyttääkö järjestelmä yhdenkään kansallisen profiilin mukaiset vähimmäisvaatimukset. Järjestelmälomakkeelle merkitään myös muut kuin profiileihin kuuluvat olennaiset vaatimukset, jotka on toteutettu järjestelmään tai täytetään järjestelmän kautta.

Sertifioinnissa tai rekisteröinnissä käytettävään järjestelmälomakkeeseen ei merkitä sellaisia järjestelmän ominaisuuksia, jotka ovat vasta suunnitteluvaiheessa tai joita ei ole toteutettu järjestelmään.

Integraatiorajapintojen tai muiden järjestelmien tai osajärjestelmien kautta täytettävät vaatimukset voidaan merkitä, jos niiden täyttyminen pystytään todentamaan osana sertifiointia.

Tietojärjestelmäpalvelun tuottajan on seurattava asiakastietolain 32 § mukaisesti olennaisten vaatimusten muutoksia ja tehtävä muutosten edellyttämät korjaukset. Jos muutokset edellyttävät uutta yhteistestausta tai uutta tietoturvallisuuden arviointia, nämä toimenpiteet on suoritettava ennen muutokset sisältävän tietojärjestelmän version tuotantokäyttöön ottamista.

Tietojärjestelmäpalvelun tuottajan on tarkistettava vähintään tietoturvallisuustodistuksen uusimiseen hakeutuessaan, että tietojärjestelmässä on yhteistestattu Kanta-palveluihin liittyvät ominaisuudet voimassa olevien määritysten ja määritysversioiden mukaisesti määräys 4/2021 luvun 10 mukaisesti.

Palvelunantaja, Kela, arviointilaitos, THL tai muu taho voi tehdä ilmoituksen Valviralle, mikäli tietojärjestelmä ei täytä tuotantokäytössä edellytettäviä olennaisia vaatimuksia.

9 Olennaisten vaatimusten täyttäminen / palvelunantaja

Asiakastietolain 34 §:n ja siinä olevien voimaantulo- ja siirtymäaikasäännösten mukaisesti palvelunantajan käyttämien tietojärjestelmien on vastattava käyttötarkoitukseltaan palvelunantajan toimintaa ja täytettävä palvelunantajan toimintaan liittyvät olennaiset vaatimukset. Olennaiset vaatimukset voidaan täyttää yhden tai useamman tietojärjestelmän tai osajärjestelmän muodostaman kokonaisuuden kautta.

Palvelunantajan on asiakastietolain 27 § ja määräyksen 3/2021 mukaisesti kuvattava tietoturvasuunnitelmassaan ne tietojärjestelmät, joita se käyttää asiakas- ja potilastietojen käsittelyyn.

Siltä osin kuin palvelunantajan toiminnassa tarvitaan kansallisten vähimmäisvaatimusten profiileissa kuvattuihin käyttötarkoituksiin käytettäviä tietojärjestelmiä, palvelunantajan tulee varmistaa, että sen käyttämät tietojärjestelmät tai osajärjestelmät kokonaisuutena toteuttavat kyseisten profiilien mukaiset vaatimukset.

Palvelunantajan on asiakastietolain mukaisia määräaikoja noudattaen liityttävä Kanta-palvelujen käyttäjäksi. Liittyminen edellyttää sitä, että palvelunantajalla on tietojärjestelmä tai tietojärjestelmäkokonaisuus, jonka kautta täytetään Kanta-palveluihin liittymisen edellytykset ja pystytään toteuttamaan palvelunantajan toiminnassa tarvittavien asiakastietojen käsittely ja tallentaminen. Liittymiseen käytettävä tietojärjestelmä voi olla luokkaan A3 kuuluva tietojärjestelmä tai järjestelmäkokonaisuus, jossa Kanta-palveluihin liittyvät vaatimukset täytetään vähintään luokkaan A2 kuuluvien tietojärjestelmien tai osajärjestelmien avulla.

Palvelunantajan tulee varmistaa, että sen käyttämät luokkaan A1, A2 tai A3 kuuluvat tietojärjestelmät on hyväksytysti sertifioitu, tuotantokäytössä näiden järjestelmien Kanta-palvelujen kautta toteutettavat ominaisuudet on hyväksytysti yhteistestattu suhteessa voimassa oleviin vaatimuksiin, ja että niitä koskeva tietoturvallisuustodistus on voimassa. Palvelunantajan on myös muilta osin pyrittävä varmistamaan, että kukin sen käyttämä tietojärjestelmä täyttää käyttötarkoituksensa mukaiset olennaiset vaatimukset. Palvelunantajan tulisi hyödyntää Valviran tietojärjestelmärekisteriä sekä hankinta- ja ylläpitosopimuksia tietojärjestelmäpalvelujen tuottajien kanssa näiden seikkojen varmistamisessa.

Palvelunantajan tulee osaltaan varmistaa, että sen toiminnassa käytettävistä luokkiin A1, A2, A3 tai B kuuluvista tietojärjestelmistä on voimassa olevat tiedot Valviran rekisterissä.

Palvelunantajan on huomioitava omassa toiminnassaan ja tietojärjestelmien käyttöönotossa, tuotantokäytössä sekä tietoturvasuunnitelman mukaisessa toiminnassa ne olennaisiin vaatimuksiin kohdistuvat huomioitavat seikat ja sertifioinnissa esiin nousseet havainnot ja edellytykset, jotka vaikuttavat olennaisten vaatimusten toteutumiseen palvelunantajan käyttämissä järjestelmissä[2]. Erityisesti on huomioitava Valviran tietojärjestelmärekisterin kautta julkaistavat tarkennukset järjestelmien vaatimustenmukaisuuden toteuttamiseen.

Palvelunantajan on asiakastietolain 27 § mukaan osana tietoturvasuunnitelmaansa osaltaan varmistettava, että tietojärjestelmän käyttöympäristö soveltuu tietojärjestelmien asianmukaiseen sekä tietoturvan ja tietosuojan varmistavaan käyttöön. Osa käyttöympäristöön kohdistuvista vaatimuksista voi toteutua tietojärjestelmäpalvelun tuottajan vastuulla olevan tietojärjestelmän kautta (ks. luku 6). Kunkin tietojärjestelmän on täytettävä ne käyttöympäristöön kohdistuvat olennaiset vaatimukset, jotka ovat tietojärjestelmäpalvelun tuottajan vastuulla. Palvelunantajan on varmistettava, että tietojärjestelmäpalvelun tuottajien ja mahdollisten muiden osapuolten kanssa on sovittu siitä, mitkä käyttöympäristön vaatimuksista täytetään kunkin osapuolen kautta.

Jos palvelunantaja toimii itse tietojärjestelmän valmistajan tai tietojärjestelmäpalvelun tuottajan roolissa, on sen täytettävä vastuullaan olevan tietojärjestelmän osalta tietojärjestelmän valmistajalle tai tietojärjestelmäpalvelun tuottajalle säädösten asettamat velvoitteet, mukaan lukien järjestelmän luokittelu, olennaisten vaatimusten täyttäminen, sertifiointi ja rekisteröinti. Tämä koskee myös mahdollisia tilanteita, joissa tietojärjestelmällä ei ole sellaista määriteltyä vastuutahoa, joka vastaa vaatimustenmukaisuudesta asiakastietolain mukaisesti. Mikäli tietojärjestelmää käyttävä palvelunantaja ei näissä tapauksissa ole sopinut tietojärjestelmää koskevien luokittelun, olennaisten vaatimusten, rekisteröinnin ja sertifioinnin vastuista, palvelunantaja vastaa näistä toimenpiteistä.

[2] Kyseessä voi olla esimerkiksi tietoturvallisuusvaatimus, jonka täyttäminen edellyttää toimenpiteitä järjestelmää käyttävän palvelunantajan käyttöympäristössä tai toiminnallinen vaatimus, jonka on täyttäminen tapahtuu järjestelmäintegraatiorajapintojen kautta.

10 Olennaisten vaatimusten todentamisen tarkennuksia

10.1 Vaatimusten täyttymisen arviointi järjestelmissä, jotka eivät liity Kanta-palveluihin

Luokkaan B kuuluville järjestelmille ei suoriteta sertifiointiin kuuluvaa yhteistestausta tai tietoturvallisuuden arviointia. Luokan A1 järjestelmille ei suoriteta yhteistestausta, mutta niille suoritetaan tietoturvallisuuden arviointi.

Luokan B tai A1 järjestelmää eivät koske Kanta-palveluihin suoraan liittyviin tietojärjestelmiin kohdistuvat yksityiskohtaiset vaatimusmäärittelyt. Suoraan säädöksistä nousevat vaatimukset asiakas- ja potilastietojen käsittelyyn koskevat myös luokan B ja A1 järjestelmiä, kuten myös luokan A2 ja A3 järjestelmiä. Olennaisten vaatimusten luokituksessa (Liite 2) on eritelty vaatimuksia, jotka nousevat suoraan keskeisimmistä asiakastietojen käsittelyä ohjaavista säädöksistä, joihin eri vaatimuksissa viitataan. Kyseisissä vaatimuksissa olevat Kanta-palveluihin liittyviä järjestelmiä koskevat määritykset ja viittaukset **eivät koske** luokan B tai A1 järjestelmiä, ellei määritysdokumentissa tai viittauksessa erikseen ole toisin ilmaistu. Näiden vaatimusten sisältö nousee luokan B ja A1 järjestelmille suoraan säännöksistä, joihin eri vaatimuksissa viitataan.

Asiakas- ja potilastietojen käsittelyyn yleisesti liittyviä vaatimuksia, jotka kohdistuvat myös luokkien B ja A1 järjestelmiin, on koottu tämän määräyksen profiililiitteeseen 3g. Nämä lakisääteiset vaatimukset kohdistuvat kaikkiin asiakas- tai potilastietojen käsittelyyn tarkoitettuihin järjestelmiin, ellei tarkemmassa järjestelmäprofiilissa ole erikseen mainittu, että vaatimus ei koske kyseisen profiilin mukaisia järjestelmiä. Lisäksi jos luokan B tai A1 järjestelmä välillisesti käyttää Kanta-palveluissa olevia tietoja tai tuottaa tietoja, jotka toimitetaan Kanta-palveluihin, sitä voivat koskea myös profiilien liitteen 3b "3b2 - Kanta-arkistointipalvelusta haettuja tietoja hyödyntävä sovellus" tai "3b4 - Kanta-arkistointipalveluun toimitettavia tietoja tuottava sovellus" vaatimukset.

Yllä mainituissa profiileissa (3g1, 3b2, 3b4) mukana olevien vaatimusten lisäksi tietojärjestelmäpalvelun tuottaja merkitsee luvun 8 mukaisesti järjestelmälomakkeeseen myös muut kuin profiileihin kuuluvat olennaiset vaatimukset, joiden mukaisia toimintoja, tietosisältöjä tai tietoturvavaatimuksia tietojärjestelmässä on toteutettu.

10.2 Vaatimusten täyttymisen arviointi ja todentamistavat sertifioinnissa

Luokan A järjestelmien sertifioinnissa (yhteistestaus ja tietoturvallisuuden arviointi) suoritetaan kunkin sellaisen järjestelmään toteutetun vaatimuksen arviointi, joka on mukana yhteistestauksen tai tietoturvallisuuden arvioinnin sisällössä. Arvioijana toimii yhteistestauksessa Kela ja tietoturvallisuuden arvioinnissa arviointilaitos.

Yksittäisen vaatimuksen osalta vaatimuksen arvioija voi ottaa kantaa vaatimuksen täyttymiseen seuraavasti:

- onko vaatimus relevantti järjestelmässä
    - relevantteja vaatimuksia ovat vähintään kaikki järjestelmän käyttötarkoitusta vastaavissa profiileissa ilmaistut pakolliset ja suositellut voimassa olevat olennaiset vaatimukset sekä ne olennaiset vaatimukset, jotka tietojärjestelmäpalvelun tuottaja on merkinnyt järjestelmään toteutetuksi toimittamassaan järjestelmälomakkeessa;
    - jos vaatimus on vain osin relevantti arvioitavan tietojärjestelmän tai osajärjestelmän osalta tai jos on tarpeen erikseen merkitä, että vaatimus ei ole järjestelmässä relevantti (esim. järjestelmän käyttötarkoitus ja käyttötarkoituksen rajaukset huomioiden), voi arvioija tehdä asiasta merkinnän arvioinnista syntyvään raporttiin, lausuntoon tai todistukseen, mikäli asiaa on tarpeen perustella;

- relevanteista vaatimuksista:
    - vaatimus täyttyy täysin (normaali tilanne);

- vaatimus ei täyty tai täyttyy vain osittain, ja täyttymättä jäävä osa kompensoidaan hyväksyttävällä tavalla siten, että vaatimuksen mukainen tavoite saavutetaan, jolloin kompensointitapa on kuvattava;
- vaatimus ei täyty;
- tarvittaessa merkintä todentamistavasta ja siitä, kuinka vaatimuksen täyttyminen on todettu, esimerkiksi viite dokumentaatioon, testausraporttiin tai ohjelmiston tuotokseen.

Yllä näkyviä tietoja voi sisältyä yksityiskohtaiseen yhteistestauksesta tai tietoturvallisuuden arvioinnista syntyvään raporttiin.

Järjestelmän käyttötarkoitukseen kuuluvien pakollisten olennaisten vaatimusten on täytyttävä tuotantokäyttöön otettavissa järjestelmissä.

Jos pakollinen olennainen vaatimus ei täyty, arvioija voi asettaa vaatimuksen täyttämiselle määräajan ennen testauksen tai tietoturvallisuuden arvioinnin hyväksymistä osana käynnissä olevaa sertifiointiprosessia.

Jos relevantti vaatimus ei täyty, mutta sen tavoite on saavutettavissa hyväksyttävästi kompensoiden, arvioija voi tehdä päätöksen hyväksymisestä siten, että hyväksyttävä kompensointi ilmoitetaan yhteistestauslausunnossa tai tietoturvallisuustodistuksessa sekä Valviran rekisterissä. Kompensoinnin hyväksyttävyyden arvioimiseksi arvioija voi edellyttää tietojärjestelmäpalvelun tuottajalta riskiarviota ja kuvausta vaatimuksen kompensoinnista. Kompensointi on poikkeuksellinen toimenpide, jonka hyväksymiseen on oltava painava peruste esimerkiksi asiakas- tai potilasturvallisuuden tai sote-palvelujen toimivuuden näkökulmasta. Kompensointi ei saa aiheuttaa haittaa tai kohtuuttomia vaatimuksia tai kustannuksia muille toimijoille. Tietojärjestelmäpalvelun tuottajan on ilmoitettava hyväksytyt kompensoinnit järjestelmää käyttäville palvelunantajille.

Jos järjestelmässä edellytettyyn vähimmäisvaatimusten profiiliin liittyvä pakollinen vaatimus ei täyty eikä vaatimusta voida hyväksyttävästi kompensoida, järjestelmä ei ole profiilin mukaiset vaatimukset täyttävä. Testausraportissa tai tietoturvallisuuden arviointiraportissa on oltava maininta asiasta. Valviran tietojärjestelmärekisteriin tehtävässä ilmoituksessa ei tule ilmoittaa profiilia, jonka mukaisia toiminnallisia tai yhteentoimivuuden vaatimuksia järjestelmä ei täytä. Järjestelmää ei tällöin saa ottaa tuotantokäyttöön kyseiseen käyttötarkoitukseen. Sitä voidaan kuitenkin käyttää niihin käyttötarkoituksiin, joihin liittyvät vaatimukset on hyväksytysti sertifioitu ja ilmoitettu. Tällöin tietojärjestelmäpalvelun tuottajan tulee osaltaan varmistaa, että järjestelmää ei käytetä käyttötarkoitukseen, jonka vaatimuksia järjestelmä ei täytä. Rajoitetusta käyttötarkoituksesta on oltava maininta Valviran tietojärjestelmärekisteriin tehtävässä ilmoituksessa ja tietojärjestelmäpalvelun tuottajan on ilmoitettava rajoitetusta käyttötarkoituksesta järjestelmää käyttäville palvelunantajille. Käyttötarkoituksen rajoitus voidaan poistaa korjausten jälkeen hyväksytyllä täydentävällä sertifioinnilla.

Kompensaatiot ja poikkeamat profiilien mukaisten pakollisten vaatimusten täyttämisestä merkitään tietoturvallisuustodistukseen, mikäli ne liittyvät tietoturvavaatimuksiin. Tietojärjestelmäpalvelun tuottajan on ilmoitettava mahdolliset kompensaatiot ja valvontaviranomaisen asettamat määräajat järjestelmää mahdollisesti käyttäville palvelunantajille.

Jos sertifioinnissa paljastuu, että jo *tuotantokäytössä toimiva* tietojärjestelmä ei täytä pakollista relevanttia vaatimusta, on tietojärjestelmä korjattava tai vaatimus kompensoitava hyväksytysti.

Valvira voi määrätä asiakastietolain mukaisen velvollisuuden määräajassa täytettäväksi (asiakastietolain 44 §). Määräaika voi koskea myös sertifiointiin liittyvää tietojärjestelmäpalvelun tuottajan tai valmistajan velvoitetta kuten korjausta tai kompensointia. Määräaika voi koskea kaikkia tuotannossa toimivan järjestelmän käyttöympäristöjä (ks. myös luku 10.4, kohta 6).

Valviran tietojärjestelmärekisterissä ilmoitetaan tietoja tuotantokäytössä olevien tietojärjestelmien poikkeamista, yhteistestauksen tuloksista ja tietoturvallisuustodistuksen voimassaolosta. Rekisterin kautta on mahdollista julkaista tietoa myös muista tietojärjestelmän käyttöön tai sertifiointiin liittyvistä seikoista kuten järjestelmän käytössä huomioitavista kompensaatioista tai rajoituksista.

Mikäli vaatimuksen toteutumisen arviointi edellyttää vaatimuksen pohjana olevan määritysdokumentin tarkempaa tulkintaa, on arvioijan tarvittaessa pyrittävä vahvistamaan tulkinta määritysdokumentin vastuutaholta kuten Kela tai THL. Vastuutahon tulisi julkaista tarkennettu tulkinta, ensisijaisti varsinaisen määritysdokumentin yhteydessä.

Tietojärjestelmäpalvelun tuottajan tulee valmistautua yhteistestaukseen tai tietoturvallisuuden arviointiin siten, että relevantit ja ei-relevantit vaatimukset on tunnistettu ja relevanttien vaatimusten täyttämisestä voidaan esittää tarvittava materiaali tai suorittaa tarvittavat todentamistoimenpiteet.

Tietoturvavaatimusten todentamisessa käytetään seuraavia todentamistapoja:

V: validointi tai tekninen tarkastus, esimerkiksi järjestelmän tuottaman lokin, sanomainstanssin tai järjestelmän tuottaman raportin läpikäynti;

testaus, jossa

TT: tarkistetaan sovellusta käyttämällä (toiminnallisella testauksella) ominaisuuden olemassaolo ja asianmukaisuus osana tietoturvallisuuden arviointia;
HT: tekninen tietoturva- ja haavoittuvuustestaus ja turvallisuustason arviointi osana tietoturvallisuuden arviointia.

D: järjestelmän dokumentaation tai muiden järjestelmään liittyvien dokumenttien läpikäynti;

(täydentävä): **H**: haastattelu osana tietoturvallisuuden arviointia, jolla voidaan syventää ja täydentää arviointia; haastattelu ei ole hyväksyttävä ensisijaiseksi vaatimuksen todentamistavaksi luokan A järjestelmissä.

Mikäli arvioitavana on olennainen tietoturvavaatimus, joka on todennettu tietojärjestelmässä muiden voimassa olevien säädösten kuin asiakastietolain nojalla kyseisissä säädöksissä hyväksytyn kolmannen osapuolen toimesta, vaatimusta ei todenneta uudelleen. Tämä edellyttää sitä, että kyseinen kolmannen osapuolen suorittama todentaminen on voimassa ja tietojärjestelmäpalvelun tuottaja esittää todentamisesta ja hyväksymisestä tarvittavan dokumentaation. Dokumentaatiosta tulee ilmetä vähintään todennetun vaatimuksen kohde riittävän tarkasti eriteltynä, säädös johon todentaminen on perustunut, todennettu vaatimus lähdeviitteineen ja vaatimuksen vastaavuus kyseiseen olennaiseen vaatimukseen, merkintä vaatimuksen hyväksytystä todentamisesta, todentaneen kolmannen osapuolen tiedot sekä voimassaolo. Esimerkkejä muiden säädösten nojalla todennetuista vaatimuksista ovat lääkinnällisten laitteiden valmistajille suoritetut laatujärjestelmän ulkoiset auditoinnit.

Vaatimusten todentamisessa on käytettävä todentamistapaa, joka on riittävä kunkin vaatimuksen tai vaatimuskohdan todentamiseen. Riittävä todentamistapa ja -taso riippuu vaatimuksesta, järjestelmän tarkemmasta luokittelusta, laajuudesta ja käyttötarkoituksesta (mm. sisällön laajuudesta ja käsiteltävien tietojen luonteesta riippuva riskitaso huomioiden). Eri vaatimusten todentamisen tapaa ja tasoa kuvataan myös tämän määräyksen liitteissä 1, 2 ja 3. Kunkin tietoturvavaatimuksen osalta Liitteessä 2 ja tarvittaessa profiileissa ilmaistaan käytettävät todentamisen tasot eri luokkiin sijoittuvissa tai eri käyttötarkoituksiin tarkoitetuissa järjestelmissä.

Tietoturvatestauksessa ja tietoturvavaatimusten todentamisessa suositellaan sovellettavaksi sopivaa yleistä tietoturvavaatimusten testauksessa käytettävää kehikkoa, kuten OWASP ASVS tai MASVS, sikäli kuin vaatimukset ovat vastaavia tai yhteensopivia liitteessä 2 esitettyjen tietoturvavaatimusten kanssa.

10.3 Vaatimusten ja määritysten versionhallinta

Tuotantokäytössä olevan tai sertifioitavan järjestelmän tulee toteuttaa kukin järjestelmään toteutettu olennainen vaatimus voimassa olevien määritysten mukaisesti, jos määritys sisältää järjestelmän luokkaa ja käyttötarkoitusta vastaavia vaatimuksia.

THL tai Kela julkaisevat tiedot siitä, mitkä ovat voimassa olevia määrityksiä ja määritysversioita, ja minkä versioiden nojalla vaatimustenmukaisuus todennetaan. Kela julkaisee ajantasaiset tiedot siitä, mitä määrityksiä ja määritysversioita edellytetään Kanta-palvelujen tuotantoympäristössä ja Kanta-rajapintoihin liittyvässä yhteistestauksessa. Luokkaan A2 tai A3 kuuluvassa tietojärjestelmässä järjestelmätoteutuksen, yhteistestauksen ja puoltavan lausunnon on perustuttava sellaisiin olennaisiin vaatimuksiin, määrityksiin ja määritysversioihin, joita kulloinkin edellytetään Kanta-palveluihin liittyvältä järjestelmältä. Kanta-palveluissa on mahdollista tukea useita määritysten versioita eri toiminnoista ja tietosisällöistä.

Jos uusien THL:n tai Kelan tuottamien määritysten tai määritysversioiden voimaantulon yhteydessä edellytetään aiemman järjestelmätoteutuksen muuttamista uutta sertifiointia vaativalla tavalla, THL tai Kela ilmaisee tämän määritysten julkaisun yhteydessä. Mikäli uudelleensertifiointia tai sertifiointitarpeen uutta arviointia edellytetään, on nämä toimenpiteet toteutettava määräyksessä tai määrityksen yhteydessä ilmaistun määräajan puitteissa. Mikäli näitä toimenpiteitä tai määräaikoja ei edellytetä, ovat myös aiempien määritysversioiden mukaiset toteutukset hyväksyttäviä testauksessa ja tuotantokäytössä.

Kela tai THL julkaisee tiedon poistuvista tai korvaantuvista määritysversioista ja siitä, mihin asti poistuvan tai korvaantuvan määritysversion mukaisia toteutuksia voidaan hyväksyä luokan A järjestelmien sertifioinnissa ja Kanta-palvelujen tuotantoympäristössä. Sosiaalihuollon asiakasasiakirjojen rakenteiden ja tietojen eri versioiden tukemiseen liittyviä vaatimuksia kuvataan THL:n määräyksessä 1/2021.

Järjestelmämuutoksista tehtäviä ilmoituksia suhteessa luokan A järjestelmien sertifiointiin käsitellään määräyksen 4/2021 liitteessä 2.

Lisätietoja määritysten hyödyntämisestä ja suhteesta olennaisiin vaatimuksiin on tämän määräyksen liitteessä 1.

10.4 Poikkeamat vaatimustenmukaisuudesta

Merkittäviä poikkeamia tuotantokäytössä toimivissa tietojärjestelmissä ovat:

1. Poikkeamat, jotka aiheuttavat riskejä potilas- tai asiakasturvallisuudelle;

2. Poikkeamat, jotka aiheuttavat merkittäviä riskejä tietosuojalle, tietoturvallisuudelle tai sosiaali- ja terveyspalvelujen toiminnalle;

3. Sellaiset poikkeamat olennaisista vaatimuksista tuotantokäytössä olevassa tietojärjestelmässä, jotka aiheuttavat merkittäviä tai pitkäaikaisia heijastusvaikutuksia tai lisäpoikkeamia useille palvelunantajille tai useille muille tietojärjestelmille;

4. Tietojen oikeellisuudelle, eheydelle tai yhteentoimivuudelle (erityisesti Kanta-palvelujen kautta) laajamittaisia häiriöitä aiheuttavat poikkeamat;

5. Tuotantokäytössä toimivan järjestelmän vaatimustenmukaisuustodistuksen tai tietoturvallisuuden arviointitodistuksen vanheneminen, erityisesti todistuksen uusimisen pitkittyessä tietojärjestelmän valmistajasta tai tietojärjestelmäpalvelun tuottajasta johtuvista syistä;

6. Tuotantokäytössä toimivassa järjestelmässä toteutettujen ominaisuuksien perustuminen vanhentuneeseen määritysversioon, jonka voimassaolo on päättynyt tai tuki Kanta-palveluissa on poistunut tai poistumassa siten, että järjestelmässä ei ole pystytty tai ei pystytä siirtymään voimassa olevien vaatimusten mukaiseen toteutukseen säännösten tai valvontaviranomaisen edellyttämässä määräajassa;

7. Säädöksissä asetettuja tai viranomaisten asettamia määräaikoja järjestelmään edellytettäville korjauksille ei ole noudatettu, erityisesti noudattamattomuuden toistuessa;

8. Muut valvontaviranomaisen (kuten Valvira, AVI tai Tietosuojavaltuutetun toimisto) merkittäväksi poikkeamaksi toteamat poikkeamat.

Merkittävistä poikkeamista on ilmoitettava asiakastietolain 41 § ja 32 § mukaisesti. Tietojärjestelmän valmistajan, tietojärjestelmäpalvelun tuottajan, välittäjän tai palvelunantajan, jota merkittävä poikkeama koskee, on ryhdyttävä toimenpiteisiin poikkeaman korjaamiseksi. Valvira julkaisee tietoa tietojärjestelmiä koskevista poikkeamista osana tietojärjestelmien rekisteriä. Valvira ohjaa ja edistää vaatimustenmukaisuutta asiakastietolain mukaisesti. Valvira voi muun muassa tehdä tarkastuksia (40 §), antaa määräyksen velvollisuuden täyttämiseksi tai puutteiden korjaamiseksi (44 § ja 45 §), asettaa käyttökiellon (45 §) sekä tehostaa antamaansa määräystä tai päätöstä uhkasakolla (49 §).

Mikäli osana sertifiointiprosessia havaitaan sellainen poikkeama olennaisista vaatimuksista, joka johtaisi merkittävään poikkeamaan tuotantokäytössä, ei sertifiointia voida hyväksytysti suorittaa loppuun ennen kuin poikkeaman aiheuttava seikka on korjattu tai poikkeamasta koituvat virhetilanteet muulla tavoin estetty.

Vaatimukset, jotka eivät täyty tai täyttyvät puutteellisesti voivat aiheuttaa korjaustarpeen ennen yhteistestauksen tai tietoturvallisuuden arvioinnin hyväksymistä, kuten luvussa 10.2 on kuvattu.

Mikäli tuotannossa toimiva tietojärjestelmä ei täytä voimassa olevia järjestelmään pakollisena kohdistuvia olennaisia vaatimuksia tai sen vaatimustenmukaisuus on vanhentunut, tietojärjestelmäpalvelun tuottajan on ilmoitettava asiasta Valviralle. Merkittävistä poikkeamista on ilmoitettava 32 § mukaisesti Valviralle ja tietojärjestelmää käyttäville palvelunantajille. Jos poikkeama johtuu tietojärjestelmästä tai tietojärjestelmäpalvelun tuottajan tai valmistajan toiminnasta, on tietojärjestelmäpalvelun tuottajan arvioitava poikkeamista koituva riski ja suunniteltava tarvittavat korjaus- tai jatkotoimenpiteet riskiarvion perusteella. Jos kyseessä on sertifioinnissa todennettu vaatimus, jonka täyttymättömyys johtuu järjestelmään tehdyistä muutoksista, on tehtävä tarvittavat muutosilmoitukset määräyksen 4/2021 liitteen 2 mukaisesti. Nämä toimenpiteet on suoritettava sen lisäksi, mitä asiakastietolain 32 § ja 41 § muuten säätävät tietojärjestelmän käyttöönoton jälkeisestä seurannasta ja poikkeamista ilmoittamisesta.

Tietojärjestelmän tai osajärjestelmän on toimittava oikeellisesti siihen toteutettujen toimintojen ja tietosisältöjen osalta. Järjestelmässä voidaan todeta olevan poikkeama olennaisista vaatimuksista, mikäli se selvästi toimii virheellisesti. Tämä ei edellytä sitä, että oikeellisuusvaatimus olisi erikseen mainittu olennaisissa vaatimuksissa tai niiden viittaamissa määrityksissä.

11 Ohjaus ja neuvonta

Lisätietoja tämän määräyksen soveltamisesta ja sertifiointiprosessista suhteessa tietojärjestelmille asetettaviin olennaisiin vaatimuksiin on liitteessä 1. Lisätietoja olennaisista vaatimuksista ja sertifiointiprosessista löytyy THL:n sivustolta ja Kanta.fi-verkkosivustolta.

Terveyden ja hyvinvoinnin laitos ohjaa ja neuvoo pyynnöstä tämän määräyksen soveltamisessa.

12 Voimaantulo ja siirtymäsäännökset

Tämä määräys tulee voimaan 9. päivänä joulukuuta 2021 ja on voimassa toistaiseksi.

Määräyksessä 4/2021 on kuvattu siirtymäsäännöksiä aiemmin sertifioitujen järjestelmien vaatimustenmukaisuuden todentamisen ja voimassaolon näkökulmasta.

Asiakastietolain edellyttämiä vaatimuksia vastaavat sosiaalihuollon tietojärjestelmäprofiilit julkaistaan vuoden 2022 alussa. Sosiaalihuollon asiakastiedon arkistoon liitettävät asiakastietojärjestelmät on sertifioitava niiden mukaisesti viimeistään silloin, kun organisaatiolla on asiakastietolain mukaan velvollisuus liittyä valtakunnalliseen arkistointipalveluun. Ennen sitä asiakastietojärjestelmiä voi sertifioida Sosiaalihuollon asiakastiedon arkiston toisen vaiheen tietojärjestelmäprofiilien mukaisesti. Ensimmäisen vaiheen profiilien mukaisia sertifikaatteja ei enää myönnetä.

Määräysten sisältämien vaatimusten voimaantulon kannalta on huomioitava *määräyksen voimaantulopäivämäärä*, josta lähtien määräystä ja sen liitteitä sovelletaan tässä ilmaistuilla tarkennuksilla ja *määräyksen 4 / 2021 siirtymäsäännöksissä ilmaistut päivämäärät*, joiden kautta ilmaistaan ennen määräysten voimaantuloa tehtyjen toimenpiteiden ja vaatimusten voimassaoloa ja jatkuvuutta, kuten aiemmin sertifioitujen järjestelmien vaatimustenmukaisuuden voimassaoloa tai määräyksen voimaan tullessa käynnissä olevien sertifiointiprosessien menettelyjä.

Profiilien ja vaatimusten toteuttamisen, sertifioinnin ja Valviran tietojärjestelmärekisteriin tehtävien ilmoitusten näkökulmasta tulee lisäksi huomioida seuraavat vaatimusten voimaantuloon liittyvät ajankohdat:

1. Määräyksen 5/2021 liitteessä olevan *profiilin voimaantulopäivä sertifioinnissa ja ilmoituksissa*, josta lähtien profiilin mukaisia vaatimuksia viimeistään sovelletaan järjestelmien sertifioinnissa (yhteistestaus ja tietoturvallisuuden arviointi) ja Valviran tietojärjestelmärekisteriin tehtävissä ilmoituksissa, jos järjestelmän käyttötarkoitus on profiilin mukainen.

2. *Profiilissa yksittäisen vaatimuksen kohdalla näkyvä päivämäärä*, joka kuvaa ajankohtaa, jolloin vaatimus on astunut tai astuu voimaan profiilin mukaisissa tuotannossa toimivissa tietojärjestelmissä. Profiilin mukaisessa tuotantokäytössä toimivassa järjestelmässä on toteutettava tai täytettävä vaatimus viimeistään tähän ajankohtaan mennessä. Jos vaatimuksen kohdalla lukee ”suositeltava”, profiilin mukaisessa järjestelmässä suositellaan vaatimuksen toteuttamista, mutta toteuttaminen ei ole tuotantokäyttöön hyväksymisen edellytys. Jos vaatimuksen kohdalla lukee ”voimassa” tai menneisyydessä oleva päivämäärä, vaatimus perustuu jo aiemmin voimassa olleisiin säännöksiin ja sen on oltava toteutettuna kaikissa tuotantokäytössä olevissa järjestelmissä, joita vaatimus koskee. Vaatimusten voimassaoloon voi kohdistua myös vaatimus- tai järjestelmäluokkakohtaisia tarkennuksia. Mahdolliset tarkennukset ilmaistaan kussakin profiilissa kunkin vaatimuksen kohdalla. Sertifioinnissa noudatetaan kohdan 1 mukaisia määräaikoja siten, että vaatimukset, joihin kohdistuu yhteistestauksen tai tietoturvallisuuden arvioinnin toimenpiteitä on todennettu ja niitä vastaava ilmoitus on toimitettu Valviran

tietojärjestelmärekisteriin ennen kuin järjestelmä tai järjestelmäversio otetaan tuotantokäyttöön. Sertifioinnissa on huomioitava vaatimukset testauksessa ja tuotantokäytössä voimassa olevien ja voimaan tulevien määritysten mukaisesti, kuten luvussa 10.3 on kuvattu.

Jos järjestelmä täyttää useiden eri profiilien mukaisia vaatimuksia, ja jollakin vaatimuksella on eri profiileissa eri voimaantuloaikoja, järjestelmässä on toteutettava vaatimus aikaisimman voimaantuloajan mukaisesti.

Myöhemmin annettavilla määräyksillä voidaan korvata tämä määräys tai täydentää sitä. Eri sosiaali- ja terveyspalveluissa erityisesti edellytettävistä olennaisista vaatimuksista tai profiileista voidaan antaa erillisiä määräyksiä. Olennaisten vaatimusten luokitusta voidaan täydentää määräystä muuttamatta erikseen ilmoitettavina ajankohtina. Uusia käyttötarkoituksia varten voidaan julkaista määräykseen ja luokitukseen perustuvia profiileja, joista voidaan tehdä sitovia uusilla määräyksillä.

Pekka Rissanen
vt. Tiedonhallintajohtaja

Jarmo Kärki
Yksikönpäällikkö

Liitteet

Liite 1. Sote-tietojärjestelmien olennaisten vaatimusten soveltamisohjeet

Liite 2. Olennaisten vaatimusten luokitus.

Liite 3a. Profiilit: Sähköisen reseptin profiilit

Liite 3b. Profiilit: Kanta-arkistointipalveluihin liittyvien järjestelmien vähimmäisvaatimukset

Liite 3c. Profiilit: Potilastiedon arkiston profiilit

Liite 3d. Profiilit: Sosiaalihuollon asiakastiedon arkiston profiilit (julkaistaan myöhemmin)

Liite 3e. Profiilit: Kuvantamisen profiilit

Liite 3f. Profiilit: Todistusten profiilit

Liite 3g. Profiilit: Asiakas- tai potilastietojen käsittelyyn tarkoitetun järjestelmän vähimmäisvaatimukset (sis. luokka B tai A1)

Liite 4: Järjestelmälomake

Jakelu

Sosiaali- ja terveydenhuollon palvelunantajat
Välittäjät
Kansaneläkelaitos
Sosiaali- ja terveydenhuollon asiakas- ja potilastietojärjestelmien valmistajat ja tietojärjestelmäpalvelujen tuottajat
Sosiaali- ja terveydenhuollon tietohallintopalvelujen ja ICT-palvelujen tuottajat
Sosiaalialan osaamiskeskukset
Sosiaali- ja terveysministeriö
Suomen Kuntaliitto ry
Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira
Lääkealan turvallisuus- ja kehittämiskeskus FIMEA
Valtiovarainministeriö
Työ- ja elinkeinoministeriö
Väestörekisterikeskus
Tietosuojavaltuutetun toimisto
Aluehallintovirastot

Tämä määräys on julkaistu viranomaisten määräyskokoelmissa:

https://www.finlex.fi/fi/viranomaiset/normi/561001/ (FINLEX® - Viranomaisten määräyskokoelmat: Terveyden ja hyvinvoinnin laitos) ja

saatavissa:

Terveyden ja hyvinvoinnin laitoksen kirjaamosta sekä

Internetosoitteesta https://thl.fi/fi/web/tiedonhallinta-sosiaalija-terveysalalla/maaraykset-ja-maarittelyt/maaraykset